UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/030,318	04/12/2002	Thomas E Rowlay III	268/207 US	5771

22249 7590 11/30/2005

LYON & LYON LLP
633 WEST FIFTH STREET
SUITE 4700
LOS ANGELES, CA 90071

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/030,318	ROWLAY, THOMAS E	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on July 05, 2005. Claims 1 – 14 are pending.

Claim Objections

2. Claims 8 – 14 are objected to because of the following informalities:

Claim 8 recites "further comprising steps performed by said host computer (12), said steps comprising:". Replace with "said verifying steps performed by said host computer (12), further comprising:" or "steps performed by said host computer (12), further comprising:".

Claim 9 recites "further comprising steps performed by said remote computer (20), said steps comprising:". Replace with "steps performed by said remote computer (20), further comprising:".

Claim number 10 is repeated.

Dependent Claims 12 – 14 cannot be dependent on the non-existing Claim 11.

Independent Claim numbered 10 should be renumbered as Claim 11.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1 – 5 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1 and 11 recite, "...a plurality of templates representing enrolled biometric information, a biometric public key....each of said plurality of templates, and ....", "...plurality of biometric templates" and Claim 5 recites "a peripheral interface (50) configured .... over a secure communication link (16)".

With respect to "a plurality of templates" and "a plurality of biometric templates", even though instant specification discloses the trusted sensor 14 selects the private key 30 unique to the enrolled template 26 (see instant application amended page 17 line 25 - page 18 line 28), the specification does not disclose "a plurality of templates" and "a plurality of biometric templates".

The dependent claims 2 – 5 and 12 – 14 are rejected at least by virtue of their dependency on the dependent claims.

With respect to "a secure communication link (16)", even though instant specification discloses "The host computer 12 is connected to a trusted sensor 14 by a data transfer bus 16, e.g., a standard RS-232 or a Universal Serial Bus ("USB") serial data interface bus" (see instant application amended page 11 lines 26 – 28) and "The functions section 32 includes a peripheral interface 50 to the host computer 12 over the bus 16, which may be a serial interface such as an RS-232, USB or a bus level bus like ISA, or PCI, with the preferred embodiment comprising an ISA interface (see instant application amended page 13 lines 1 – 3), the specification does not disclose "a secure communication link".

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 9 recites the limitation "said remote computer (20)" in lines 1 and 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1 – 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Bjorn et al. (U.S. Patent Number 6,122,737).

6. Regarding Claim 1, Bjorn teaches a microprocessor (34); a data memory (36) coupled to said microprocessor (34) and configured to hold a plurality of templates representing enrolled biometric information, a biometric public key private key pair corresponding to each of said plurality of templates, and a manufacturer public key and private key pair (Column 4 lines 21 – 25); and

a functions section (32) coupled to said microprocessor (34), said functions section comprising:

a cryptographic library module (60) storing one or more public key private key encryption functions and further storing instructions for causing said microprocessor (34) to populate said biometric public key and private key pair corresponding to each of said plurality of templates (Column 4 lines 44 – 47);

a feature extraction and template matching module (58) storing instructions for causing said microprocessor (34) to extract features created with a biometric image capture device (24) coupled to said trusted sensor (14) and to populate to at least one of said plurality of templates, and further storing instructions for causing said microprocessor (34) to match sensed biometric information, communicated from said

biometric image capture device (24), to said enrolled biometric information stored said data memory (36) and, based on said match, select a particular biometric private key (Column 4 lines 44 – 62); and

an authentication module (56) storing instructions for causing said microprocessor (34) to certify said trusted sensor (14) to a host computer by executing said one or more encryption functions stored in said cryptographic module (60) using said manufacture private key and a host computer public key (Column 4 lines 44 – 62).

7. Regarding Claim 6, Bjorn teaches

performing a power on self-test on said trusted sensor (14); verifying said on said trusted sensor (14) to a host computer (12) coupled to said trusted sensor (14), said step of verifying using a manufacturer private key (40) and a host computer public key (42) (Column 4 lines 44 – 47);

receiving biometric information from an image capture device (24); matching said biometric information from said image capture device (24) to an enrolled biometric template (26) stored in said trusted sensor (14) (Column 4 lines 44 – 47);

selecting a public key (28) and a private key (30) pair corresponding to said enrolled biometric template (26), said public key (28) and private key (30) pair stored in said trusted sensor (14) (Column 4 lines 44 – 47);

receiving a message from said host computer (12), said message including a remote computer public key (46); encrypting at least a portion of said message using said selected private key (30) and said remote computer public key (46); and sending

said encrypted message form said trusted sensor (14) to said host computer (12) (Column 3 lines 37 – 56 and Column 4 lines 44 – 47).

8. Regarding Claim 11, Bjorn teaches

a remote computer (20) including a remote computer public key (46) and private key (48) pair; a host computer (12) coupled to said remote computer (20), said host computer (12) including a host computer public key (42) and private key (44) pair (Column 4 lines 44 – 47 and Column 5 lines 2 – 15);

a biometric image sensing means (24) including a plurality of capacitive sensing elements for measuring relative distances between ridges and valleys on a fingerprint (Column 4 lines 44 – 47); and

a trusted sensor (14) coupled to said biometric image sensing means (24) and said host computer (12), said trusted sensor (14) including a microprocessor (34), a functions section (32) accessible by said microprocessor (34), and a data memory (36) including a plurality of biometric templates (26), each of said plurality of biometric templates (26) having a biometric template public key (28) and private key (30) pair, and a manufacturer public key (38) and private key (40) pair, wherein biometric information sensed by said biometric image sensing means (24) is manipulated and stored in said plurality of biometric templates (26), and wherein each of said biometric template public key (28) and private key (30) pairs is dependent upon said manipulated biometric information stored in corresponding one of said plurality of biometric templates (26) (Column 3 lines 37 – 56; Column 4 lines 44 – 47 and Column 5 lines 1 – 40).

9. Claim 2 is rejected applied as above in rejecting Claim 1. Furthermore, Bjorn teaches authentication module (56) further storing instructions for causing said microprocessor (34) to execute said one or more encryption functions stored in said cryptographic library module (60) using said particular biometric private key, a public key corresponding to a remote computer, said one or more encryption functions encrypting a message destined for said remote computer (Column 3 lines 37 – 56; Column 4 lines 44 – 47 and Column 5 lines 1 – 40).

10. Claim 3 is rejected applied as above in rejecting Claim 2. Furthermore, Bjorn teaches wherein said biometric image capture device (24) includes a plurality of capacitive fingerprint sensing elements; and

wherein said manufacturer public key and private key pair correspond to said plurality of capacitive fingerprint sensing elements (Column 3 lines 37 – 56; Column 4 lines 44 – 47 and Column 5 lines 1 – 40).

11. Claim 4 is rejected applied as above in rejecting Claim 2. Furthermore, Bjorn teaches wherein said biometric image capture device (24) includes a plurality of capacitive fingerprint sensing elements; and

wherein said manufacturer public key and private key pair correspond to said functions section (32) (Column 3 lines 37 – 56; Column 4 lines 44 – 47 and Column 5 lines 1 – 40).

12. Claim 5 rejected applied as above in rejecting Claims 3 or 4. Furthermore, Bjorn teaches said functions section further comprising:

a power on self-test and tamper detect feature (62) storing instructions for causing said microprocessor (34) to enable said trusted sensor (14) when said power on self-test is successful and said tamper detected feature detects no tampering (Column 4 lines 44 – 47);

a secure time stamp module (52) storing instructions for causing said microprocessor (34) to generate a time stamp used by said authentication module (56); and a peripheral interface (50) configured to communicatively couple microprocessor (50) to said host computer over a secure communications link (16) (Column 7 lines 11 – 18).

13. Claim 7 is rejected applied as above in rejecting Claim 6. Furthermore, Bjorn teaches said step of verifying comprising:

receiving an encrypted random number from said host computer (12), said encrypted random number encrypted by said host computer (12) using a host computer private key (44) and a manufacturer public key (38) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

decrypting said encrypted random number into a random number using said host computer public key (42) and said manufacturer private key (40) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

modifying said random number; encrypting said modified random number using said manufacturer private key (40) and said host computer public key (42); and sending said encrypted modified random number to said host computer (12) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

14. Claim 8 is rejected applied as above in rejecting Claim 7. Furthermore, Bjorn teaches steps performed by said host computer (12), said steps comprising:

generating said random number; encrypting said random number using said host computer private key (44) and said manufacturer public key (38) to form said encrypted random number; sending said encrypted random number to said trusted sensor (14) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving said encrypted modified random number from said trusted sensor (14); decrypting said encrypted modified random number using said host computer private key (44) and said manufacturer public key (38); and verifying said modification performed by said trusted sensor (14) to said random number (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

15. Claim 9 is rejected applied as above in rejecting Claim 8. Furthermore, Bjorn teaches further comprising steps performed by said remote computer (20), said steps comprising:

encrypting a primary message with a remote computer private key (48) and a transaction public key, said transaction public key selected from a group comprising

said host computer public key (28) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving a confirmation message from said host computer (12), said confirmation message comprising said portion of said message encrypted at said trusted sensor (14) using said selected private key (30) and said remote computer public key (46) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63); and

decrypting said portion of said confirmation message using said selected transaction key and said remote computer private key (48) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

16. Claim 10 is rejected applied as above in rejecting Claims 6 – 9. Furthermore, Bjorn teaches one or more computer readable mediums having stored therein one or more sequences of instructions for causing one or more microprocessors to perform the steps (Column 3 line 63 – Column 4 line 4).

17. Claim 12 rejected applied as above in rejecting Claim 10. Furthermore, Bjorn teaches wherein said trusted sensor (14) is verified by host computer (12) by:

sending a first message from said host computer (12) to said trusted sensor (14), said first message encrypted with said host computer private key (44) and said manufacturer public key (38) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving said first message at said trusted sensor (14), decrypting said first message, manipulating a portion of said first message, returning a return first message to said host computer (12), said return first message including said manipulated portion of said first message and said return first message encrypted with said manufacturer private key (40) and said host computer public key (42) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63); and

receiving said return first message from said trusted sensor (14) at said host computer (12), decrypting said return first message with said host computer private key (44) and said manufacturer public key (38) and verifying said manipulation to said portion of said first message (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

18. Claim 13 is rejected applied as above in rejecting Claim 12. Furthermore, Bjorn teaches wherein a transaction is verified, after first verifying said trusted sensor (14), by:

sensing current user biometric information using said biometric image sensing means (24); comparing said current user biometric information to said plurality of biometric templates (26) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

selecting a particular biometric image template that matches said current user biometric information, said act of selecting including identifying a particular biometric public key and private key pair corresponding to said particular biometric image template (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

encrypting a second message authorizing a transaction with said particular biometric private key and said remote computer public key (46); sending said second message to said host computer (12) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

receiving said second message from said trusted sensor (14) at said host computer (12); re-transmitting said second message from host computer (12) to said remote computer (20) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63); receiving said re-transmitted second message from host computer (12) at said remote computer (20); and verifying said re-transmitted second message using said host computer private key (48) and said particular biometric public key (Column 5 lines 25 – 32 and Column 6 lines 45 – 63).

19. Claim 14 is rejected applied as above in rejecting Claim 13. Furthermore, Bjorn teaches wherein prior to said step of re-transmitting said second message, and host computer encrypts said second message using said host computer private key (44) and said remote computer public key (46) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63); and

wherein said step of verifying said re-transmitted second message includes verifying said second message using said host computer public key (42) (Column 5 lines 25 – 32 and Column 6 lines 45 – 63);

Conclusion

20. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz

Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
November 26, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100